DEVICE AND SYSTEM FOR PREVENTING COMPUTER VIRUS INVASION

Patent Number: JP5108487

Publication date: 1993-04-30

Inventor(s): MURAKAMI SEIJI

Applicant(s): SEIJI MURAKAMI

Requested Patent: JP5108487

Application Number: JP19910292322 19911011

Priority Number(s):

IPC Classification: G06F12/14; G06F12/16

EC Classification:

Equivalents: JP8023846B

Abstract

PURPOSE:To previously check invasion of computer virus and to prevent its invasion and proliferation by discriminating whether the request taken into by a request taking-in means is a correct request or the one by computer virus.

CONSTITUTION:A virus monitoring system A is selectively present between an application 3 and an operating system 5. The monitoring system A fetches the content of request 9 by using a request fetching means 15. Then, a requested content discriminating means 17 discriminates whether the requests 9 fetched is a correct one or the one by computer virus. When the request is the one from computer virus, an outputting means 19 rejects its request and also issues an alarm. A virus monitoring systems B and C, being present between the application and a basic BIOS 7 and a hardware 1, respectively, work similarly. These monitoring systems A-C are not the same type and selectively incorporated in.

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平5－108487

(43)公開日　平成5年(1993)4月30日

(51)Int.Cl.⁵	識別記号	庁内整理番号	FI	技術表示箇所
G06F 12/14	310 A	9293－5B		
12/16	310 B	7629－5B		

審査請求　有　請求項の数2　(全9頁)

(21)出願番号　特願平3-292322

(22)出願日　平成3年(1991)10月11日

(71)出願人　591249242
村上　清治
静岡県静岡市川辺町2丁目2番16号

(72)発明者　村上　清治
静岡県静岡市川辺町二丁目2番16号

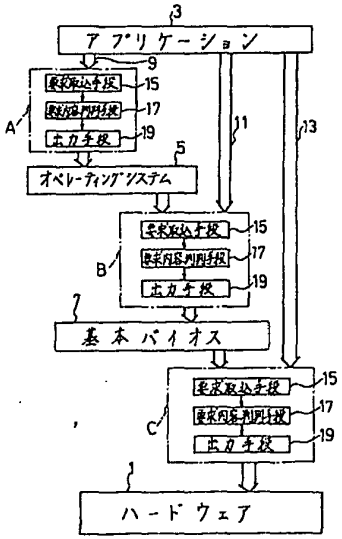
(74)代理人　弁理士　島野　英伊智

(54)【発明の名称】コンピュータウイルス侵入防止装置と侵入防止方式

(57)【要約】

【目的】　コンピュータウィルスの侵入を事前にチェックして、その侵入・増殖を防止することを可能とするコンピュータウィルス侵入防止装置と侵入防止方式を提供することを目的とする。

【構成】　例えば、アプリケーションプログラムからオペレーティングシステムへの要求を取り込み、取り込まれた要求が正常な要求か又はコンピュータウィルスによる要求かを判別し、判別結果に基づいて該要求がコンピュータウィルスによる要求の場合に少なくともその要求を禁止するようにしたものである。



1

【特許請求の範囲】

【請求項1】　アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求、の内、少なくとも一箇所においてその要求を取り込む要求取込手段と、上記要求取込手段によって取り込まれた要求が正常な要求か又はコンピュータウィルスによる要求かを判別する要求内容判別手段と、上記要求内容判別手段の判別結果に基づいて該要求がコンピュータウィルスによる要求の場合に少なくともその要求を禁止する出力手段と、を具備したことを特徴とするコンピュータウィルス侵入防止装置。

【請求項2】　アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求の内、少なくとも一箇所においてその要求を取り込み、上記取り込まれた要求が正常な要求か又はコンピュータウィルスによる要求かを判別し、上記要求内容がコンピュータウィルスによる要求の場合に少なくともその要求を禁止するようにしたことを特徴とするコンピュータウィルス侵入防止方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、コンピュータウィルス侵入防止装置と侵入防止方式に係り、特に、コンピュータウィルスが侵入して増殖する前に、これを事前にチェックしてその侵入・増殖を防止できるものに関する。

【0002】

【従来の技術】昨今、コンピュータウィルスによるプログラムの破損が大きな社会問題となっている。ここに、コンピュータウィルスとは、自己増殖能力及び感染能力を持ち、ネットワーク或いはフロッピーディスクを通して、他のコンピュータに侵入する悪性のプログラムをいう。この種のコンピュータウィルスの感染経路としては、上記したように、ネットワークを通じて侵入したり、既にコンピュータウィルスに汚染されたフロッピーディスクを使用することにより感染するものである。コンピュータウィルスに感染した場合には、画面上に不必要なメッセージが表示されたり、システムエラーが異常に増えたり、記憶されているファイルが消去されたり、場合によってはハードディスクが破損してしまうといった症状が発生することになる。

【0003】このようなコンピュータウィルスの侵入・増殖に対して、従来は次のような方法により対処していた。まず、各種ファイルに外からの書込みを禁止する書込禁止操作を施して、コンピュータウィルスのファイルへの侵入を防止する方法がある。又、コンピュータウィルスが感染していない正常なファイルを常備しておき、この正常なファイルと使用するファイルとを比較することにより、ファイルの感染の有無を確認するという方法がある。さらに、ファイル操作の履歴を作成し、その履歴を調べることによりコンピュータウイルスに感染されているか否かを判別する方法もある。

2

【0004】

【発明が解決しようとする課題】上記従来の構成によると次のような問題があった。コンピュータウィルスの侵入・増殖に対する従来の方策は、全て事後的なものであった。すなわち、ファイルを任意の方法により直接操作して、コンピュータウィルスの感染の有無を確認するものであり、これでは、コンピュータウィルスの侵入・増殖を事前に防止することはできず、仮に、従来の方法によりコンピュータウィルスの感染の事実を確認できても、その時には、既に広く蔓延してしまっているという可能性もあった。

【0005】本発明はこのような点に基づいてなされたものでその目的とするところは、コンピュータウィルスの侵入を事前にチェックして、その侵入・増殖を防止することを可能とするコンピュータウィルス侵入防止装置と侵入防止方式を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するべく本願発明によるコンピュータウィルス侵入防止装置は、アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求の内、少なくとも一箇所においてその要求を取り込む要求取込手段と、上記要求取込手段によって取り込まれた要求が正常な要求か又はコンピュータウィルスによる要求かを判別する要求内容判別手段と、上記要求内容判別手段の判別結果に基づいて該要求がコンピュータウィルスによる要求の場合に少なくともその要求を禁止する出力手段と、を具備したことを特徴とするものである。

【0007】又、本発明によるコンピュータウィルス侵入防止方式は、アプリケーションプログラムからオペレーティングシステムへの要求、アプリケーションプログラムから基本バイオスへの要求、アプリケーションプログラムからハードウェアへの要求の内、少なくとも一箇所においてその要求を取り込み、上記取り込まれた要求が正常な要求か又はコンピュータウィルスによる要求かを判別し、上記要求内容がコンピュータウィルスによる要求の場合に少なくともその要求を禁止するようにしたことを特徴とするものである。

【0008】

【作用】本発明の場合には、アプリケーションからオペレーティングシステム又は基本バイオス又はハードウェアへの要求の内少なくとも一箇所において、その要求を取り込む。次に取り込んだ要求が正常なものか或いはコンピュータウィルスによって汚染されたものかを判別す

る。判別した結果、コンピュータウィルスによって汚染されたものである場合には、要求を禁止するようにしたものである。

【０００９】以下、図１ないし図１２を参照して本発明の一実施例を説明する。まず、図１を参照して本実施例による装置及び方式の概略を説明する。通常、各種コンピュータ及びそれを動かすソフトウェアにおいては、まず、ハードウェア１がある。このハードウェア１は、コンピュータシステムを構成する機器そのそものであり、図では省略してあるが、コンピュータ本体、ディスプレイ、プリンタ、外部記憶装置、通信機器等を意味している。

【００１０】上記ハードウェア１に対してソフトウェアがあり、このソフトウェアによって上記ハードウェア１に指令を送って所望の動作を行わせるものである。上記ソフトェアとしては、図に示すように、アプリケーション（アプリケーションプログラム）３、オペレーティングシステム５、基本バイオス７がある。上記アプリケーション３は、通常、応用プログラムと称されており、コンピュータを使用する本来の目的のためのプログラムである。又、オペレーティングシステム５は、基本プログラムの一つであり、コンピュータのハードウェア１及びソフトウェアを有効に利用するために総合管理を行うものである。さらに、上記基本バイオス７は、コンピュータの基本動作を収めたプログラム群のことであり、ハードウェア１を制御するためのものである。そして、上記アプリケーション３は、オペレーティングシステム５、基本バイオス７、ハードウェアー１を適宜呼び出したり操作したりして、所望の動作を行わせることになる。

【００１１】上記アプリケーション３からオペレーティングシステム５には任意の要求９が出力される。同様に、アプリケーション３から基本バイオス７に対しても任意の要求１１が出力されるとともに、アプリケーション３からハードウェア１に対しても任意の要求１３が出力される。

【００１２】上記アプリケーション３とオペレーテイングシステム５との間には、ウィルス監視システムＡが選択的に介在するようになっている。このウイルス監視システムＡは、要求９の内容を要求取込手段１５によって取込み、取り込んだ要求９が正常なものか或いはコンピュータウィルスによるものかを要求判別手段１７によって判別し、判別の結果、仮に、コンピュータウィルスによる要求である場合には、出力手段１９によってアプリケーション３からオペレーティングシステム５に対する要求を禁止するとともに警告を出力するものである。又正常な場合にはオペレーティングシステム５に実行を移すことになる。尚、上記警告としては、画面上にメッセージを表示したり、或いは、ブザーを鳴らすようなことが考えられる。

【００１３】又、アプリケーション３と基本バイオス７との間には、ウィルス監視システムＢが選択的に介在するようになっている。さらに、アプリケーション３とハードウェア１との間には、ウィルス監視システムＣが選択的に介在するように構成されている。これらウィルス監視システムＢ及びウィルス監視システムＣも、上記ウィルス監視システムＡの場合と同様に、要求取込手段１５によって要求１１又は１３を取込み、取り込んだ要求１１又は１３を要求判別手段１７によって判別し、その判別の結果、コンピュータウィルスによる要求である場合には、出力手段１９によって要求を禁止するとともに警告を出力するものである。

【００１４】次に、上記ウィルス監視システムＡ、Ｂ、Ｃが、コンピュータの電源を投入してから、どのような手順でシステム内に組み込まれていくかについて、図２を参照して説明してみる。まず、電源を投入して「開始」となる。次に、ハードウェア１に合ったウィルス監視システムＣが導入されるとともに、基本バイオス７の整備が行われる。次に、基本バイオス７の整備が完了したか否かの判別がなされる。基本バイオス７の整備が完了した場合には、基本バイオス７に合ったウィルス監視システムＢが導入される。又、基本バイオス７の整備が完了していない場合には、再度基本バイオス７の整備を行う。

【００１５】次に、オペーレーティングシステム５の整備を行う。オペレーティングシステム５の整備が完了した場合には、オペレーティングシステム５に合ったウィルス監視システムＡを導入する。オペレーティングシステム５の整備が完了していない場合には、再度オペレーテイングシステム５の整備を行う。そして、ウイルス監視システムＡの導入が完了した時点で、システムの組み込みが完了することになり、アプリケーション３からの要求を監視する体制ができたことになる。又、既に述べたように、ウイルス監視システムＡ、Ｂ、Ｃのそれぞれは、一種類ではなく、ハードウェア１、基本バイオス７、オペレーティングシステム５の種類によって任意の種類のものを選択して組み込むことになる。尚、本実施例においては、かかる一連の処理を図示しないＲＯＭ上に記録するようにしている。それによって、コンピュータウィルスによる書換えを防止するようにしている。

【００１６】次に、ウィルス監視システムＡ、Ｂ、Ｃとして、具体的にどのような方式が採られるかについて説明していく。まず、データベース法（スキャン法）から説明する。これは、各種のコンピュータウィルスによるコンピュータプログラムを予めデータベース化して配憶しておき、それが検査対象になっているコンピュータプログラムに存在するか否かを判別していくものである。以下、図３を参照して説明する。まず、要求取込手段１５によって要求を取り込む。次に、取り込んだ要求を解析して、判断が必要か否かを判別する。判断が必要でない場合にはそのまま処理が続行される。一方、判断が必要な場合には、予め配憶されているデータベースのデータとの比較が行われる。そして、要求とデータベース化されたデータとが一致していない場合には、そのまま処理が続行される。又、要求とデータベース化されたデータとが一致している場合には、要求が禁止されるとともに警告・問い合わせが行われる。次に、処理が確認され続行するか否かが判別される。続行しないと判断した場合には、プロセスが中断されることになる。

【００１７】上記データベース化されたデータとの比較・判別をさらに詳しく示すと、図４に示すようなものとなる。まず、ファイルの読み込みが行われる。次に、データベースの中から最初のデータを取り出す。そして、読み込んだファイル内容と取り出したデータとを比較して一致するか否かを判別する。一致している場合には、「ＳＴＣ」、すなわち、コンピュータウィルスに感染されているものと判断する。一方、一致していない場合には、データベースの中の全てのデータと比較したか否かが判別される。全てのデータと比較した場合には、「ＣＬＣ」、すなわち、正常であると判断される。全てのデータと比較していない場合には、次のデータとの比較が行われる。すなわち、データベースの中から次のデータを取り出して、読み込んだファイルとの比較を行っていく。このようにして、データベースの全てのデータと比較していくことにより、コンピュータウィルスの感染の有無を判別していくものである。

【００１８】次に、バックアップ法による判別について、図５及び図６を参照して説明する。バックアップ法とは、検査対象となっているファイルのバックアップファイルを予め作成・保存しておく。すなわち、ファイルの全部又は一部又はファイル内容を加工した情報をバックアップファイルとして予め作成・保存しておくものである。後は、検査対象のファイルと上記バックアップファイルとを比較して正常であるか否かを判別していくものである。

【００１９】以下、図を参照して詳細に説明すると、まず、図５に示すように、バックアップファイルの作成を開始する。つまり、ファイルの内容を読み込んでＳＵＭ計算、すなわち、ファイルのバイトの合計値を計算する。そして、ＳＵＭデータを出力して、そのＳＵＭ計算とファイル名とをバックアップファイル（ディスク）に記録しておく。これによって、バックアップファイルその作成が完了する。

【００２０】次に、上記予め作成されているバックアップファイルを使用したバックアップ法による判別を図６を参照して説明する。まず、検査対象のファイルからデータを読み込む。次に、読み込んだデータに基づいてＳＵＭ計算を行う。次に、計算された値とバックアップファイルから取り込んだ計算値とを入力して、一致するか否かの判別がなされる。そして、一致していない場合には、「ＳＴＣ」、すなわち、コンピュータウィルスに感染されているものと判断される。又、一致している場合には、「ＣＬＣ」、すなわち、正常であると判断される。

【００２１】次に、図７乃至図１０を参照して接種法を採用した場合について説明する。この接種法とは、検査対象になるファイルに、ウィルスの感染の有無を判別するプログラムを予め接種しておき、システム起動時において、ファイル自身にウィルスの感染の有無を判別させるものである。まず、通常のファイル２１は、図７に示すようになっていて、本来の元プログラム２３だけが記録されている。このファイル２１にＳＵＭデータ２５とチェックプログラム２７を接種して、接種済ファイル２９を作成する。この接種ファイル２９の作成工程を示したのが図９である。すなわち、元プログラムファイルの読み込みが行われ、次に、ＳＵＭ計算が行われる。次に、ファイルの末尾にＳＵＭデータが付加されるとともに、チェックプログラムが付加される。そして、ファイルの先頭をチェックプログラムにジャンプして、接種ファイル２９の作成が完了する。

【００２２】次に、接種ファイル２９が自身でコンピュータウィルスの感染の有無をどのような工程で判別していくかについて説明する。図１０に示すように、接種ファイル２９を実行すると、チェックプログラムが起動する。そして、その時点で、元プログラム２３のＳＵＭを計算し、その計算値と、予め記録されているＳＵＭ値とを比較する。そして、一致している場合には正常であるとして、元プログラム２３を起動する。これに対して、一致しない場合には、元プログラム２３がウィルスに汚染されているとして、以降の実行を中止するものである。

【００２３】次に、キーワード法を採用した場合について説明する。このキーワード法とは、特定の動作をキーワードによって禁止する方法であり、任意のキーワードを使用してキーワードが一致した場合に以降の動作を許可するというものである。以下、図１１を参照して説明する。これは、ＭＳ－ＤＯＳ（登録商標）のサービスの中のファイル番込要求に対して行う場合を示すものであり、まず、番込要求（ＡＨ＝４０）が出される。次に、パスワード検査が行われ、パスワードが一致しない場合には、ウィルスに感染されているものと判断し、一致している場合には正常であると判断される。

【００２４】次に、手続法を採用した場合について説明する。すなわち、コンピュータウィルスに汚染されている場合と、正常な場合とでは、プロセスに違いがある。これをチェックすることにより、コンピュータウィルスに感染されているか否かを判別するものである。具体的には、例えば、ＭＳ－ＤＯＳ（登録商標）のサービス要求の中にファイル番込可能オープン要求（ＡＸ＝３Ｄ０２）を要求する場合、正常な場合にはファイルの属性を要求することはないが、コンピュータウィルスに汚染さ

7

れている場合には、直前にファイルの属性変更（ＡＸ＝４３０１）を要求してくる。よって、上記ファイルの属性変更を要求するか否かによって、コンピュータウィルスに汚染されているか否かを判別することができる。上記手続法の一例を図１２に示す。

【００２５】尚、ウィルス監視システムＡ、Ｂ、Ｃにおいて、上記したような各方法の中からどの方法を採用して行うかについては任意であり、又、それら以外の別の方法を採用してもよい。

【００２６】以上本実施例によると次のような効果を奏することができる。まず、アプリケーション３からコンピュータウィルスによって汚染された要求が出された時点でこれをチェックし、コンピュータウィルスに汚染されているか否かを判別して、汚染されている場合には要求を中止させるとともに警告を出力するように構成しているので、アプリケーション３がコンピュータウィルスによって汚染されているか否かを早期に発見することができるとともに、以降のコンピュータウィルスの侵入・蔓延を事前に防止することができる。特に、コンピュータウィルスによる汚染の有無の確認をシステム内で自動的に行うようにしているので、従来のように事後的にチェックするのとは異なり、コンピュータウィルスの侵入・蔓延による被害を最小限に食い止めることができる。

【００２７】又、使用するオペレーティングシステム５、基本バイオス７、ハードウェアー１によって、適切なウィルス監視システムＡ、Ｂ、Ｃを自動的に選択して投入できるようになっているので、使いがっても良好である。

【００２８】尚、本発明は前記一実施例に限定されるものではない。例えば、前記一実施例では、図１に示すように、アプリケーション３、オペレーティングシステム５、基本バイオス７、ハードウェアー１のそれぞれの間に、ウィルス監視システムＡ、Ｂ、Ｃを介在させるようにしたが、それらの中から任意の箇所に介在させるだけの構成も考えられる。

【００２９】

【発明の効果】以上詳述したように本発明によるコンピュータウィルス侵入防止装置と侵入防止方式によると、コンピュータウィルスによる汚染の有無を早期に発見して、それ以降の侵入・蔓延を未然に防止することができる。よって、従来のような事後的な方法に比べて、コンピュータウィルスによる被害を大幅に軽減させることができる。

8

【図面の簡単な説明】

【図１】本発明の一実施例を示す図でコンピュータウィルス侵入防止装置の構成を示すブロック図である。

【図２】本発明の一実施例を示す図でウィルス監視システムの導入を示すフローチャートである。

【図３】本発明の一実施例を示す図でデータベース法による判別を示すフローチャートである。

【図４】本発明の一実施例を示す図でデータベース法による判別を示すフローチャートである。

【図５】本発明の一実施例を示す図でバックアップ法による判別を示すフローチャートである。

【図６】本発明の一実施例を示す図でバックアップ法による判別を示すフローチャートである。

【図７】本発明の一実施例を示す図で接種法による判別において元のファイルを模式的に示す図である。

【図８】本発明の一実施例を示す図で接種法による判別において接種ファイルを模式的に示す図である。

【図９】本発明の一実施例を示す図で接種法による判別において接種の工程を示すフローチャートである。

【図１０】本発明の一実施例を示す図で接種法による判別を示すフローチャートである。

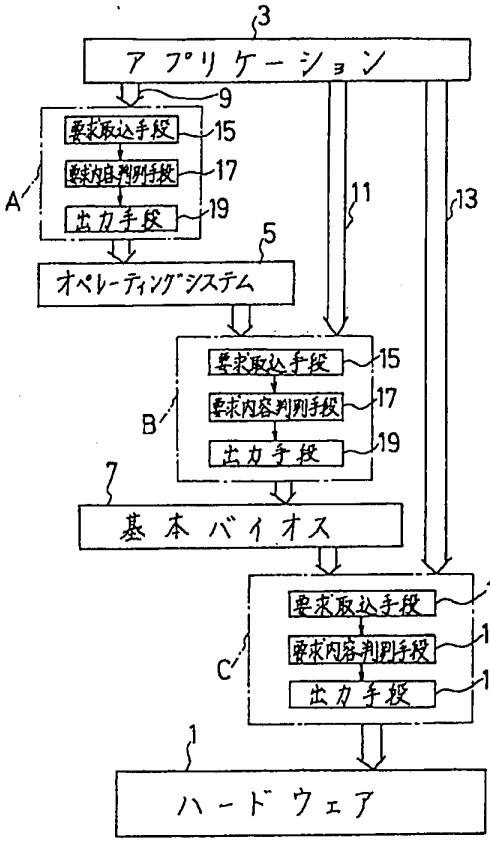
【図１１】本発明の一実施例を示す図でパスワード法による判別を示すフローチャートである。

【図１２】本発明の一実施例を示す図で手続法による判別を示すフローチャートである。

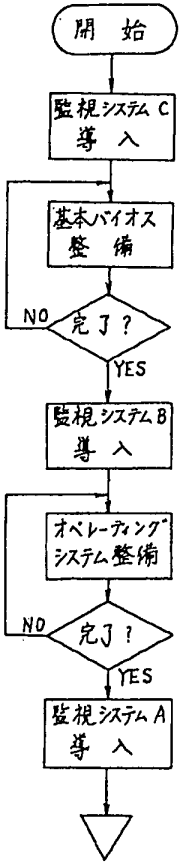
【符号の説明】

１　ハードウェア
３　アプリケーション
５　オペレーティングシステム
７　基本バイオス
９　要求
１１　要求
１３　要求
１５　要求取込手段
１７　要求内容判別手段
１９　出力手段
Ａ　ウィルス監視システム
Ｂ　ウィルス監視システム
Ｃ　ウィルス監視システム

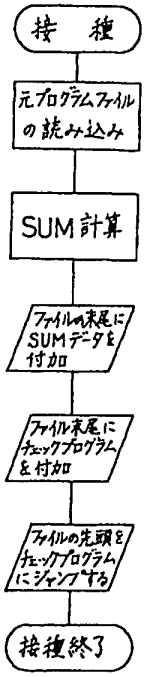
【図１】



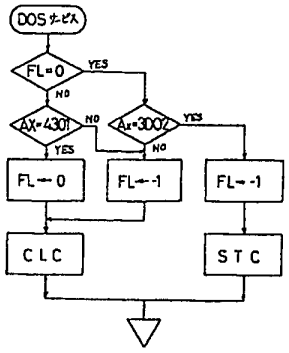
【図２】



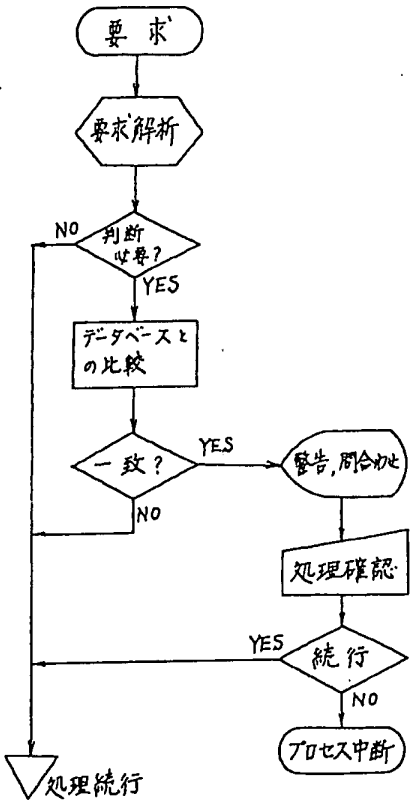
【図９】



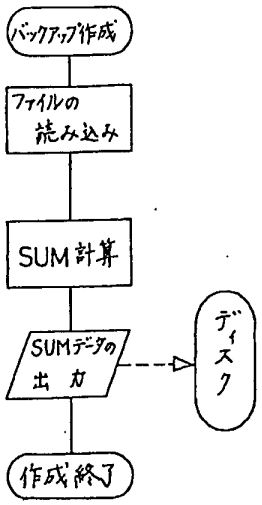
【図１２】



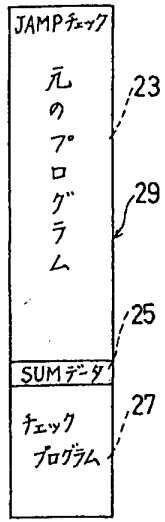
【図3】



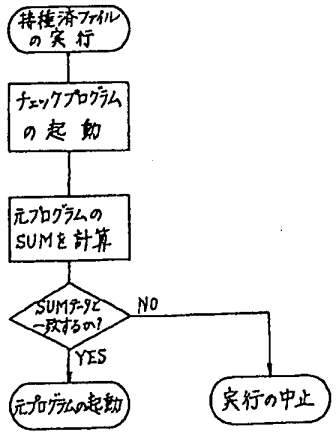
【図5】



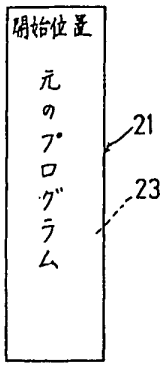
【図8】



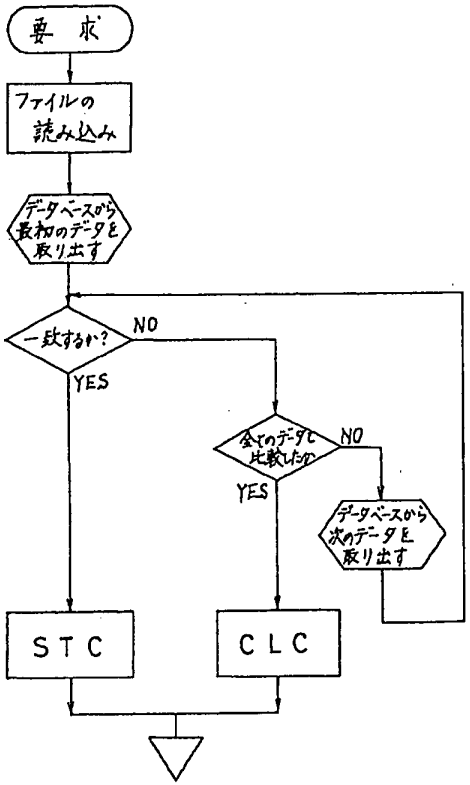
【図10】



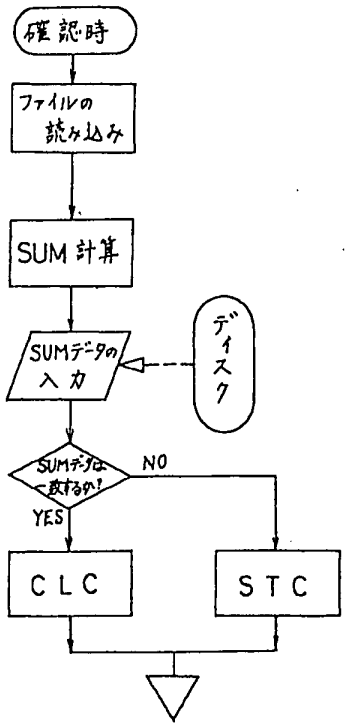
【図7】



【図4】



【図6】



【図11】